Application No.: 10/680,400
Attorney Docket No: 14846-28

Reply Under 37 CFR 1.116
Expedited Procedure
Tech. Center: 2131

REMARKS

Introduction

Claims 1-12 were pending. Claims 1, 11, 12, and 13 are independent. Claims 1 and 10 have been amended. Claim 13 has been added. Claims 2, 4, 5, 11, and 12 have been cancelled.

Applicant notes with appreciation the courtesies extended by Examiner Zia during the telephonic interview conducted on September 18, 2007. In the interview, Examiner Zia and applicant discussed amendments to claim 1 to narrow the preamble such that a subsequent search of the prior art would consequently be narrowed. Also discussed was an amendment to claim 1 to better explain what happens when a user logs into a privileged account unsuccessfully and to add limitations to claim 1 to more faithfully reflect the flow chart steps of FIGS. 2 and 3 of the present application. As described in further detail below, applicant has herein amended the claims in accordance with the discussions during the interview.

Rejections under 35 U.S.C. § 112

The Examiner (Jackson) rejected claim 12 under 35 U.S.C. § 112, first and second paragraph. By the cancellation of claim 12 herewith, the rejection of Claim 12 is obviated. Thus, applicant respectfully requests that the rejection of claim 12 be withdrawn.

Application No.: 10/680,400
Attorney Docket No: 14846-28

Reply Under 37 CFR 1.116
Expedited Procedure
Tech. Center: 2131

Rejections under 35 U.S.C. § 103(a)

Claims 1-10 stand rejected under 35 U.S.C. 103(a) as unpatentable over U.S. Patent Application Publication No. 2004/0148259 (Reiners et al.) in view of U.S. Patent Application Publication No. 2004/0068559 (Shaw).

Reiners et al. describes a transaction authorization system for access to online banking accounts. The online bank account may include, for example, an electronic or virtual credit card account, an electronic or virtual debit card account, or the like. To prevent fraudulent access to the account, the user is provided with the ability to "enable" or "disable" the account. By "enabled" is meant that transactions performed using the bank account are authorized, and by "disabled" is meant that transactions performed using the bank account are unauthorized. The account holder enables or disables the account via an account status database. The account holder enables or disables their account by logging into an account administrative server, during which the account holder is authenticated by entering a correct username and password (see page 2, paragraph [0034], or FIG. 3, block 54). Alternatively, the account administrative server may require identification via a smart card, digital certificate, or via biometric data, such as a fingerprint. The account holder enables or disables an account based on a pre-selected condition, such as a specified time period or a predetermined event, such as a maximum number of attempted logins. A third party merchant, at a later date, may attempt to access the account for the purpose of a bank transaction. The transaction is authorized in a convention fashion by checking account balance or credit lint, but in addition, the transaction may take place only if the account is "enabled."

In contrast to the system described by Reiners et al., amended claim 1 of the present application recites, *inter alia*, a method for allowing a user to temporarily gain access to a

Application No.: 10/680,400
Attorney Docket No: 14846-28

Reply Under 37 CFR 1.116
Expedited Procedure
Tech. Center: 2131

privileged account on a computer system to perform a maintenance task, the method being a replacement for a conventional switch user command, comprising: receiving a switch user command login with a user id and an account name as an argument; retrieving a list of privileged account names; determining whether the account name is in a list of privileged account names and diverting the user to the conventional switch user command prompt if the account name is not in the privileged account list; otherwise, determining whether the user id belongs to a privileged group having permission to access privileged accounts; denying access to privileged accounts and notifying the manager if the user id does not belong to the privileged group, otherwise, allowing access to the account; prompting for a reason for accessing the account; recording a reason for accessing the account; notifying a manager by email of the access of the privileged account of the switch user login along with the name of a first log file; recording keystrokes in the first log file while logged into the account; recording keystrokes in a duplicate log file while logged into the account; determining whether the first log file was tampered with and, if so, recording that the first log file was tampered with in the duplicate log file and transmitting the duplicate log file to the manager; terminating the switch user login; and notifying the manager by email of the privileged account of the switch user login termination.

Reiners et al. does not teach or suggest receiving a switch user command login containing an account name and user id, nor checking whether the account name is in a list of privileged account names and diverting the user to the conventional switch user command prompt if the account name is not in the privileged account list. In addition, Reiners et al. does not describe prompting for a reason for accessing the account nor recording a reason for accessing the account. While t\The Examiner contends that recording a reason for accessing the account can be found at Reiners et al., paragraphs [0020, 0021], these paragraphs merely state that the system

Application No.: 10/680,400
Attorney Docket No: 14846-28

Reply Under 37 CFR 1.116
Expedited Procedure
Tech. Center: 2131

may contain an authentication facility for authenticating the identity of the bank holder via an account holder interface. The account holder interface accesses and interrogates the account status database to obtain a transaction record or statement. Nowhere is it specified or suggested that the user is prompted to enter a reason for using an account. Elsewhere in Reiners et al., as described above, the account holder is authenticated by entering a correct username and password (see page 2, paragraph [0034], or FIG. 3, block 54). Alternatively, the account administrative server may require identification via a smart card, digital certificate, or via biometric data, such as a fingerprint. In the "Response to Amendment" section of the present Office Action, the Examiner contends that the reason for accessing the account is located in paragraph [0109] of Reiners et al. as "to get account details of the online bank account". The user is, without prompting, requesting account details. There is no mention of a computer system prompting interactively for a reason which can change with the specific maintenance task to be performed. Nor does Reiners et al. describe recording a prompted for reason, as is also recited by claim 1 of the present application.

Furthermore, at paragraph [0022] and [0122] of Reiners et al., the user can *optionally* enter notes for the login after having been granted login access, which is not a required entering of a reason for accessing an account before being granted access.

Moreover, Reiners et al. also does not teach or suggest notifying a manager of the privileged account of a successful login; nor does Reiners et al. teach or suggest notifying the manager when the login is terminated. Indeed, the Examiner does not cite any part of Reiners et al. for a successful login notification, and for the termination, cites paragraph [0116] of Reiners et al. Paragraph [0116] merely states that the user can notify the administration server of the disabling of an account, not its successful login or termination of a login to an account. The

Application No.: 10/680,400
Attorney Docket No: 14846-28

Reply Under 37 CFR 1.116
Expedited Procedure
Tech. Center: 2131

Examiner admits that Reiners et al. does not disclose recording keystrokes in a log file. Specifically with regard to independent claim 1, as amended, Reiners et al. does not teach or disclose logging keystrokes in a duplicate file, and determining whether the first log file was tampered with and, if so, recording that the first log file was tampered with in the duplicate log file and transmitting the duplicate log file to the manager. Reiners et al. does not teach or disclose determining whether the user id belongs to a privileged group located in a group list on the computer system (as in a Unix-like group id portion of file permissions associated with a file) having permission to access privileged accounts and denying access to privileged accounts and notifying the manager if the user id does not belong to the privileged group. Reiners et al. at paragraph [0110] discloses that, optionally, the user can be verified by a third party on another computer system via the web as to whether the user belongs to a trusted community associated with the second computer system. There is no lookup in a group list on the same computer system as is used for logging into a privileged account.

Accordingly, applicant submits that Reiners et al. does not teach or suggest several of the limitations recited by amended claim 1 of the present application.

Shaw fails to correct the deficiencies of Reiners et al. Shaw describes a method for detecting unauthorized computer system usage by monitoring a user's activities, such as keystrokes, uploading bytes, or downloading bytes. The unauthorized activity may be recorded in an activity log or may be terminated by the computer system. However, Shaw fails to disclose recording the same keystrokes in a duplicate file and placing a notification of tampering with a first log file into the duplicate log file.

Further, there is no mention anywhere in Shaw of the process of a user logging into an account, and whether this login process includes prompting for and receiving a reason for

Application No.: 10/680,400
Attorney Docket No: 14846-28

Reply Under 37 CFR 1.116
Expedited Procedure
Tech. Center: 2131

logging into the account. Still further, there is no mention in Shaw of receiving a switch user command and diverting execution to the traditional switch user command if an entered account name is not in the privileged account list. There is no mention in Shaw of checking if a user belongs to a privileged group in a group list.

Accordingly, applicant submits that neither Reiners et al. nor Shaw, alone or in combination, teaches or suggests the invention recited by amended claim 1 of the present application. As such, withdrawal of the rejection of claim 1 under 35 U.S.C. 103(a) based on Reiners et al. in view of Shaw is requested.

Each of claims 3 and 6-10 ultimately depend from claim 1, that has been shown to be patentable, and is likewise deemed to be patentable, for at least the reasons described above with respect to the patentability of claim 1.

New claim 13 recites the limitations of claim 1, prior to the present amendments, but with the preamble amended to conform to that of claim 1 as presently amended, and with the limitation of a specific invocation of a switch user command and the result of unsuccessfully logging into the switch user command. Applicants submit that new claim 13 is patentable over Reiners et al. and Shaw, either taken alone, or in combination.

Thus, applicant submits that each of the claims of the present application are patentable over each of the references of record, either taken alone, or in any proposed hypothetical combination. Accordingly, withdrawal of the rejections to the claims is respectfully requested.

Application No.: 10/680,400
Attorney Docket No: 14846-28

Reply Under 37 CFR 1.116
Expedited Procedure
Tech. Center: 2131

Conclusion

In view of the above remarks, reconsideration and allowance of the present application is respectfully requested. No fee is believed to be due in connection with this Amendment. If, however, other fees are deemed necessary for this Amendment to be entered and considered by the Examiner, then the Commissioner is authorized to charge such fee to Deposit Account No. 50-1358. Applicant's undersigned patent agent may be reached by telephone at (973) 597-2500. All correspondence should continue to be directed to our address listed below.

Respectfully submitted,

Date: _9/28/07_

Raymond G. Cappo
Patent Agent for Applicant
Registration No. 53,836

DOCKET ADMINISTRATOR
LOWENSTEIN SANDLER PC
65 Livingston Avenue
Roseland, NJ 07068